US-PAT-NO: 7028338
DOCUMENT-IDENTIFIER: US 7028338 B1

TITLE: System, computer program, and method of cooperative response to threat to domain security

DATE-ISSUED: April 11, 2006

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Norris; James W.	Kansas City	MO		US
Everson; John	Kansas City	MO		US
LaMastres; Daniel	Independence	MO		US

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Sprint Spectrum L.P.	Overland Park	KS		US	02

APPL-NO: 10/023558 [PALM]
DATE FILED: December 18, 2001

ABSTRACT:

A system, computer program, and method of providing an automatic cooperative response ability to all members of a domain in light of a detected threat or other suspicious activity, such as, for example, a virus or denial of service attack, directed, at least initially, at less than all members of the domain. The system broadly comprises the domain; a log server; a detection server; and a profile server. The domain comprises a logical grouping of members having similar risk profiles. The detection server monitors and parses log and audit records generated by the members and copied to the log server. When the detection server identifies threatening or other suspicious activity it sets an alert status in a security profile stored on the profile server. The members periodically query the profile server for updates to the alert status and are thereby apprised of the alert.

My interpretation
log server = proxy loghost
detection server = central loghost
profile server = monitoring station